



US006226387B1

(12) **United States Patent**
Tewfik et al.(10) **Patent No.:** US 6,226,387 B1(45) **Date of Patent:** May 1, 2001(54) **METHOD AND APPARATUS FOR
SCENE-BASED VIDEO WATERMARKING**(75) **Inventors:** Ahmed H. Tewfik, Edina; Mitchell D.
Swanson, Minneapolis; Bin Zhu, St.
Paul, all of MN (US)(73) **Assignee:** Regents of the University of
Minnesota, Minneapolis, MN (US)(*) **Notice:** Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.(21) **Appl. No.:** 08/921,931(22) **Filed:** Aug. 27, 1997**Related U.S. Application Data**(60) Provisional application No. 60/050,587, filed on Jun. 24,
1997, and provisional application No. 60/024,979, filed on
Aug. 30, 1996.(51) **Int. Cl.⁷** G06K 9/00(52) **U.S. Cl.** 382/100(58) **Field of Search** 382/100, 232;
380/210, 287, 54(56) **References Cited****U.S. PATENT DOCUMENTS**

3,395,024	7/1968	Earle	99/169
4,313,197	1/1982	Maxemchuk	370/111
4,425,661	1/1984	Moses et al.	375/1
4,495,620	1/1985	Steele et al.	370/118
4,969,041	11/1990	O'Grady et al.	358/142
5,010,405	4/1991	Schreiber et al.	358/141
5,060,262	10/1991	Bevins, Jr. et al.	380/19
5,285,498	2/1994	Johnston	381/2
5,315,098	5/1994	Tow	235/494
5,319,735	6/1994	Peuss et al.	395/2.14
5,325,290	6/1994	Cauffman et al.	364/401
5,379,345	1/1995	Greenberg	380/23
5,386,240	1/1995	Hori	348/473
5,404,377	4/1995	Moses	375/200
5,450,490	9/1995	Jensen et al.	380/6

5,461,426	10/1995	Limberg et al.	348/475
5,465,269	11/1995	Schaffner et al.	375/200
5,465,308	11/1995	Hutcheson et al.	382/159
5,473,631	12/1995	Moses	375/202
5,515,296	5/1996	Agarwal	364/514 R
5,530,759	6/1996	Braudaway et al.	380/54

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

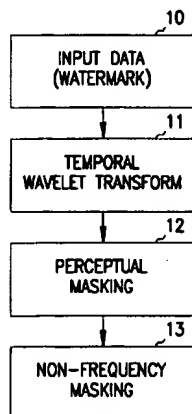
0581317A2	2/1994	(EP)	G07D/7/00
0 635 798 A1	1/1995	(EP)	G06F/17/30
0635798A1	1/1995	(EP)	G06F/17/30
0 657 831 A1	6/1995	(EP)	G06F/17/30
0657831A1	6/1995	(EP)	G06F/17/30
07-160731	6/1995	(JP)	G06F/17/30

OTHER PUBLICATIONSOhnishi et al., "Embedding a Seal into a Picture under
Orthogonal Wavelet Transform," IEEE Proc. 3rd Int. Conf.
on Multimedia Computing and Systems, Jun. 17-23, 1996,
pp. 514-521.*Aizawa, K., "Model-Based Image Coding", *Proceedings of
the SPIE, Visual Communications and Image Processing '94*
vol. 2308, Chicago, IL, 1035-1049 (Sep. 25-29, 1994).

(List continued on next page.)

Primary Examiner—Andrew W. Johns(74) **Attorney, Agent, or Firm**—Schwegman, Lundberg,
Woessner & Kluth P.A.(57) **ABSTRACT**

A method and apparatus for the scene-based watermarking of video data is disclosed. In one embodiment, each of a number of frames of a scene of video host data undergoes a temporal wavelet transform, from which blocks are extracted. The blocks undergo perceptual masking in the frequency domain, such that a watermark is embedded therein. Once the watermark block is taken out of the frequency domain, a spatial mask of the original block is weighted to the watermark block, and added to the original block to obtain the watermarked block.

14 Claims, 5 Drawing Sheets

U.S. PATENT DOCUMENTS

5,579,471	11/1996	Barber et al.	395/326
5,583,941	12/1996	Yoshida et al.	380/51
5,606,609	2/1997	Houser et al.	380/4
5,613,004	3/1997	Cooperman et al.	380/28
5,646,997	7/1997	Barton	380/23
5,687,236	11/1997	Moskowitz et al.	380/28
5,710,719	1/1998	Houle	364/514 R
5,710,916	1/1998	Barbara et al.	395/609
5,809,139	9/1998	Girod et al.	380/5
5,848,155	12/1998	Cox	380/4
5,850,481	12/1998	Rhoads	382/232
5,859,920	1/1999	Daly et al.	382/115
5,905,819 *	5/1999	Daly	382/284
5,915,027 *	6/1999	Cox et al.	380/54
5,930,369 *	7/1999	Cox et al.	380/54

OTHER PUBLICATIONS

- Baritaud, T., et al., "On the Security of the Permuted Kernel Identification Scheme", *Proceedings of the 12th Annual International Cryptology Conference, Advances in Cryptology—Crypto '92*, Brickell, E.F., (ed.), Santa Barbara, CA, 305–311 (Aug. 16–20, 1992).
- Bender, W., et al., "Techniques for Data Hiding", *IBM Systems Journal*, 35, 313–336 (1996).
- Bender, W., et al., "Techniques for Data Hiding", *SPIE*, 2420, 164–173 (1995).
- Boland, F.M., et al., "Watermarking Digital Images for Copyright Protection", *IEEE International Conference on Image Processing and Its Applications*, Edinburgh, Scotland, 326–330 (Jul. 4–6, 1995).
- Boney, L., et al., "Digital Watermarks for Audio Signals", *Proceedings of the 1996 IEEE International Conference on Multimedia Computing and Systems, Multimedia '96*, Hiroshima, Japan, 473–480 (Jun. 1996).
- Bors, A.G., et al., "Image Watermarking Using DCT Domain Constraints", *Proceedings of the 1996 IEEE International Conference on Image Processing*, vol. III, Lausanne, Switzerland, 231–234 (Sep. 16–19, 1996).
- Bouman, C., et al., "Multiple Resolution Segmentation of Textured Images", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 13, 99–113 (Feb. 1991).
- Cawkell, A.E., "Picture-Queries and Picture Databases", *The Journal of Information Science*, 19, 409–423 (1993).
- Chalom, E., et al., "Segmentation of an Image Sequence Using Multi-Dimensional Image Attributes", *Proceedings of the 1996 IEEE International Conference on Image Processing*, vol. II, Lausanne, Switzerland, 525–528 (Sep. 16–19, 1996).
- Chan, W.-Y., et al., "Generalized Product Code Vector Quantization: A Family of Efficient Techniques for Signal Compression", *Digital Signal Processing*, 4, 95–126 (1994).
- Chang, S.-F., "Compressed-Domain Techniques for Image/Video Indexing and Manipulation", *Proceeding of the 1995 IEEE International Conference on Image Processing*, vol. 1, Washington, D.C., 314–317 (Oct. 23–26, 1995).
- Chang, S.-F., et al., "Transform Coding of Arbitrarily-Shaped Image Segments", *Proceedings of the ACM, Multimedia 93*, Anaheim, CA, 83–90 (Aug. 1–6, 1993).
- Chitprasert, B., et al., "Human Visual Weighted Progressive Image Transmission", *IEEE Transactions on Communications*, 38, 1040–1044 (Jul. 1990).
- Corset, I., et al., "MPEG-4: Very Low Bit Rate Coding for Multimedia Applications", *Proceedings of the SPIE, Visual Communications and Image Processing '94*, vol. 2308, Chicago, IL 1065–1073 (Sep. 25–29, 1994).
- Cox, I.J., et al., "Secure Spread Spectrum Watermarking for Images, Audio and Video", *Proceedings of the 1996 IEEE International Conference on Image Processing*, vol. III, Lausanne, Switzerland, 243–246 (Sep. 16–19, 1996).
- Craver, S., et al., "Can Invisible Watermarks Resolve Rightful Ownership!", *IBM Research Technical Report, RC 20509, IBM CyberJournal*, 23 p. (Jul. 25, 1996).
- Daubechies, I., et al., "Orthonormal Bases of Compactly Supported Wavelets", *Communications on Pure and Applied Mathematics*, XLI, 909–996 (Oct. 1988).
- Faloutsos, C., et al., "Signature Files: An Access Method for Documents and Its Analytical Performance Evaluation", *ACM Transactions on Office Information Systems*, 2, 267–288 (Oct. 1984).
- Flickner, M., et al., "Query by Image and Video Content: The QBIC System", *Computer*, 28, 23–32 (Sep. 1995).
- Gary, J.E., et al., "Shape Similarity-Based Retrieval in Image Database Systems", *Proceedings of the SPIE, Image Storage and Retrieval Systems*, vol. 1662, San Jose, CA, 2–8 (Feb. 13–14, 1992).
- Girod, B., "The Information Theoretical Significance of Spatial and Temporal Masking in Video Signals", *Proceedings of the SPIE, Human Vision, Visual Processing and Digital Display*, vol. 1077, 178–187 (1989).
- Gruber, J., "Smart Paper", *Wired*, 2, 46 (Dec. 1994).
- Gudivada, V.N., et al., "Content-Based Image Retrieval Systems", *Computer*, 28, 18–22 (Sep. 1995).
- Hartung, F., et al., "Digital Watermarking of Raw and Compressed Video", *SPIE*, 2952, 205–213 (Oct. 1996).
- Hirata, K., et al., "Rough Sketch-Based Image Information Retrieval", *NEC Research & Development*, 34, 463–473 (Apr. 1993).
- Hirotsugu, K., "An Image Digital Signature System with ZKIP for the Graph Isomorphism", *Proceedings of the 1996 IEEE International Conference on Image Processing*, vol. III, Lausanne, Switzerland, 247–250 (Sep. 16–19, 1996).
- Hsu, C.-T., et al., "Hidden Signatures in Images", *Proceedings of the 1996 IEEE International Conference on Image Processing*, vol. III, Lausanne, Switzerland, 223–226 (Sep. 16–19, 1996).
- Huang, Z., et al., "Affine-Invariant B-Spline Moments for Curve Matching", *IEEE Transactions on Image Processing*, 5, 1473–1480 (Oct. 1996).
- Huffman, D.A., "A Method for the Construction of Minimum-Redundancy Codes", *Proceedings of the IRE*, 40, 1098–1101 (1952).
- Jacobs, C.E., et al., "Fast Multiresolution Image Querying", *Proceedings of the ACM, SIGGRAPH Conference on Computer Graphics*, Los Angeles, CA, 277–286 (1995).
- Jayant, N., et al., "Signal Compression Based on Models of Human Perception", *Proceedings of the IEEE*, 81, 1385–1422 (Oct. 1993).
- Johnston, J.D., et al., "Wideband Coding—Perceptual Considerations for Speech and Music", In: *Advances in Speech Signal Processing*, Furui, S., et al., (eds.), Dekker, New York, p. 109–140 (1992).
- Le Gall, D., "MPEG: A Video Compression Standard for Multimedia Applications", *Communications of the ACM*, 34, 46–58 (Apr. 1991).

- Legge, G.E., et al., "Contrast Masking in Human Vision", *The Journal of the Optical Society of America*, 70, 1458-1471 (Dec. 1980).
- Lin, H.-C., et al., "Color Image Retrieval Based on Hidden Markov Models", *Proceedings of the 1995 IEEE International Conference on Image Processing vol. 1*, Washington, D.C., 342-345 (1995).
- Macq, B.M., et al., "Cryptology for Digital TV Broadcasting", *Proceeding of the IEEE*, 83, 944-957 (Jun. 1995).
- Manjunath, B.S., et al., "Browsing Large Satellite and Aerial Photographs", *Proceedings of the 1996 IEEE International Conference on Image Processing, vol. II*, Lausanne, Switzerland, 765-768 (Sep. 16-19, 1996).
- Matsui, K., et al., "Video-Steganography: How to Secretly Embed a Signature in a Picture", *IMA Intellectual Property Project Proceedings, vol. 1*, 187-206 (Jan. 1994).
- Nam, J., et al., "Combined Audio and Visual Streams Analysis for Video Sequence Segmentation", *Proceedings of the 1997 IEEE International Conference on Acoustics, Speech and Signal Processing, vol. IV*, Munich, Germany, 2665-2668 (Apr. 21-24, 1997).
- Niblack, W., et al., "The QBIC Project: Querying Images by Content Using Color, Texture and Shape", *Proceedings of the SPIE, Storage and Retrieval for Image and Video Databases, vol. 1908*, 173-187 (1993).
- Nill, N.B., "A Visual Model Weighted Cosine Transform for Image Compression and Quality Assessment", *IEEE Transactions on Communications, COM-33*, 551-557 (Jun. 1985).
- Noll, P., "Wideband Speech and Audio Coding", *IEEE Communications Magazine*, 31, 34-44 (Nov. 1993).
- O Ruanaidh, J.J.K., et al., "Phase Watermarking of Digital Images", *Proceedings of the 1996 IEEE International Conference on Image Processing vol. III*, Lausanne, Switzerland, 239-242 (Sep. 16-19, 1996).
- Pitas, I., "A Method for Signature Casting on Digital Images", *Proceedings of the 1996 IEEE International Conference on Image Processing, vol. III*, Lausanne, Switzerland, 215-218 (Sep. 16-19, 1996).
- Rioul, O., et al., "Wavelets and Signal Processing", *IEEE Signal Processing Magazine*, 8, 14-38 (Oct. 1991).
- Rivest, R.L., "Cryptography", In: *Handbook of Theoretical Computer Sciences*, vol. A, Van Leeuwen, J., (ed.), p. 717-755 (1990).
- Rivest, R.L., et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM* 21, 120-126 (Feb. 1978).
- Smith, J.P., "Authentication of Digital Medical Images with Digital Signature Technology", *Radiology*, 194, 771-774 (Mar. 1995).
- Smith, J.R., et al., "Modulation and Information Hiding in Images", *Information Hiding*, Proceedings of the First Int. Workshop, Anderson, R., (ed.), Cambridge, U.K., 207-226 (May 30-Jun. 1, 1996).
- Srihari, R.K., "Combining Text and Image Information in Content-Based Retrieval", *Proceedings of the 1995 IEEE International Conference on Image Processing*, Washington, D.C., 326-328 (Oct. 23-26, 1995).
- Strang, G., "Wavelets and Dilation Equations: A Brief Introduction", *SIAM Review*, 31, 614-627 (Dec. 1989).
- Swain, M.J., et al., "Color Indexing", *International Journal of Computer Vision*, 7, 11-32 (1991).
- Tanaka, K., et al., "Embedding Secret Information into a Dithered Multi-Level Image", *1990 IEEE Military Communications Conference, vol. 1*, "Milcom 90: A New Era," Monterey, CA, 216-200 (Sep. 30-Oct. 3, 1990).
- van Schyndel, R.G., et al., "A Digital Watermark", *Proceedings of the IEEE, ICIP-94, vol. II*, Austin, TX, 86-90 (Nov. 13-16, 1994).
- Voyatzis, G., et al., "Applications of Toral Automorphisms in Image Watermarking", *Proceedings of the 1996 IEEE International Conference on Image Processing, vol. II*, Lausanne, Switzerland, 237-240 (Sep. 16-19, 1996).
- Wallace, G.K., "The JPEG Still Picture Compression Standard", *Communications of the ACM*, 34, 30-44 (Apr. 1991).
- Witten, I.H., et al., "Arithmetic Coding for Data Compression", *Communications of the ACM*, 30, 520-540 (Jun. 1987).
- Wolfgang, R.B., et al., "A Watermark for Digital Images", *Proceedings of the 1996 IEEE International Conference on Image Processing, vol. III*, Lausanne, Switzerland, 219-222 (Sep. 16-19, 1996).
- Wunsch, P., et al., "Wavelet Descriptors for Multiresolution Recognition of Handprinted Characters", *Pattern Recognition*, 28, 1237-1249 (Aug. 1995).
- Zhu, B., et al., "Image Coding with Mixed Representations and Visual Masking", *Proceedings of the 1995 IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 4*, Detroit, MI, 2327-2330 (May 9-12, 1995).
- Zhu, B., et al., "Low Bit Rate Near-Transparent Image Coding", *Proceedings of the SPIE, International Conference on Wavelet Applications for Dual Use, vol. 2491*, Orlando, FL, 173-184. (1995).
- Zhu, S.C., et al., "Region Competition: Unifying Snakes, Region Growing, Energy/Bayes/MDL for Multi-band Image Separation", *Proceedings of the IEEE Fifth International Conference on Computer Vision*, Massachusetts Institute of Technology, Cambridge, MA, 416-423 (Jun. 20-23, 1995).
- Ziv, J., et al., "A Universal Algorithm for Sequential Data Compression", *IEEE Transactions on Information Theory*, IT-23, 337-343 (May 1977).

* cited by examiner

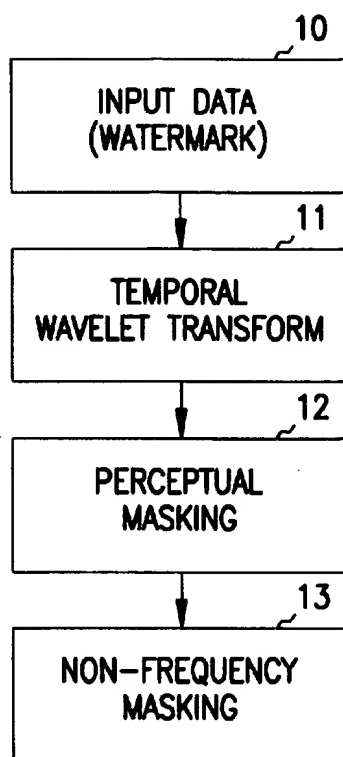


FIG. 1

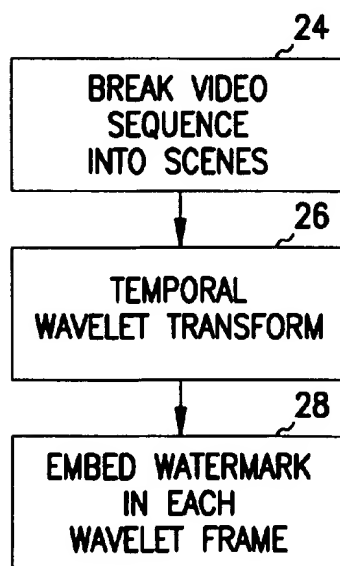


FIG. 2

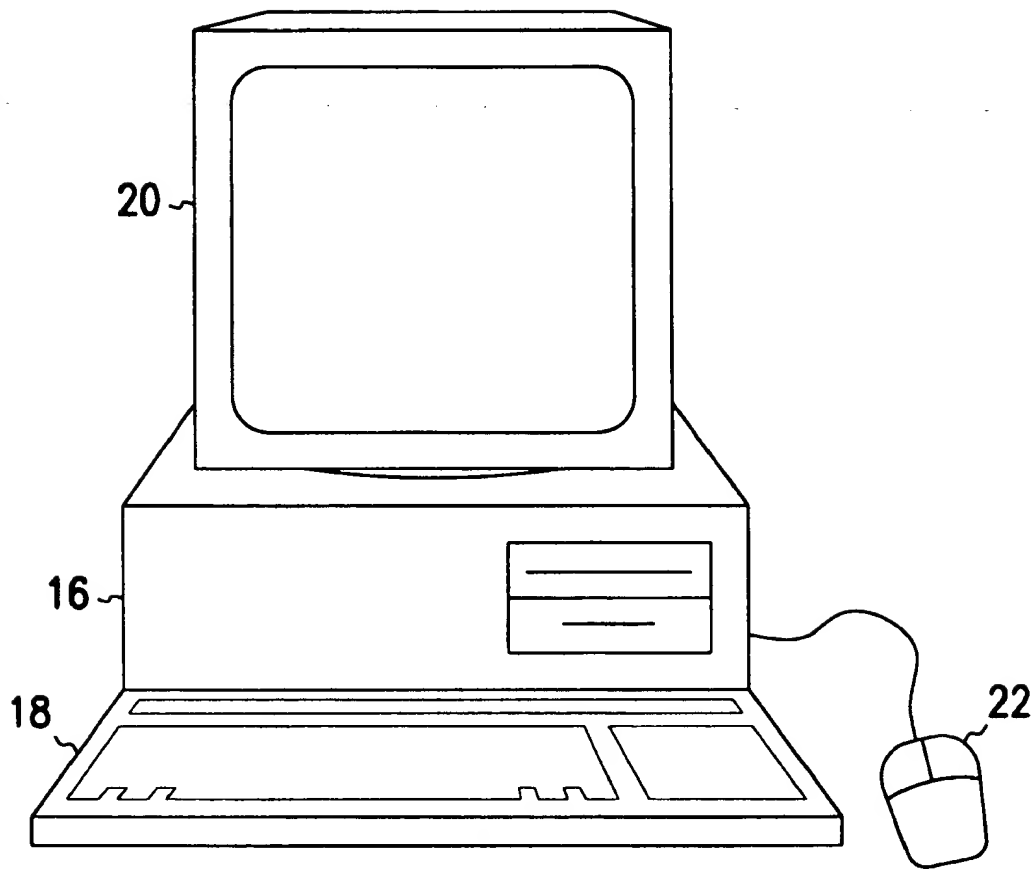


FIG. 3

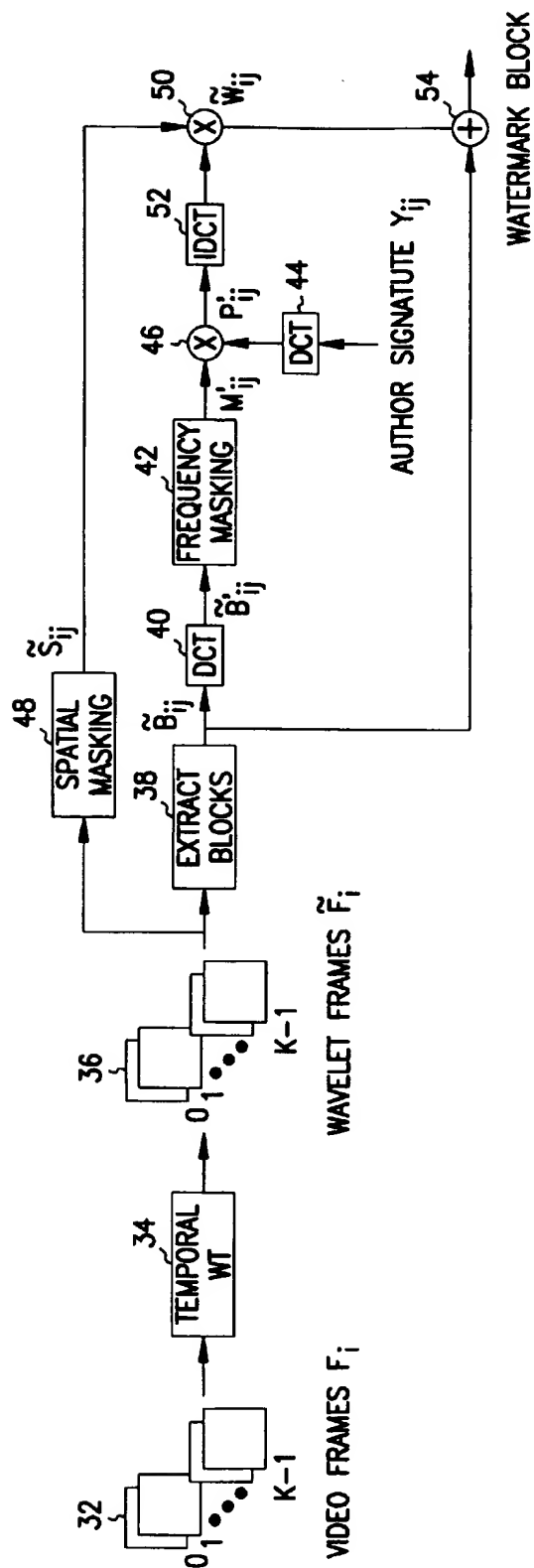


FIG. 4

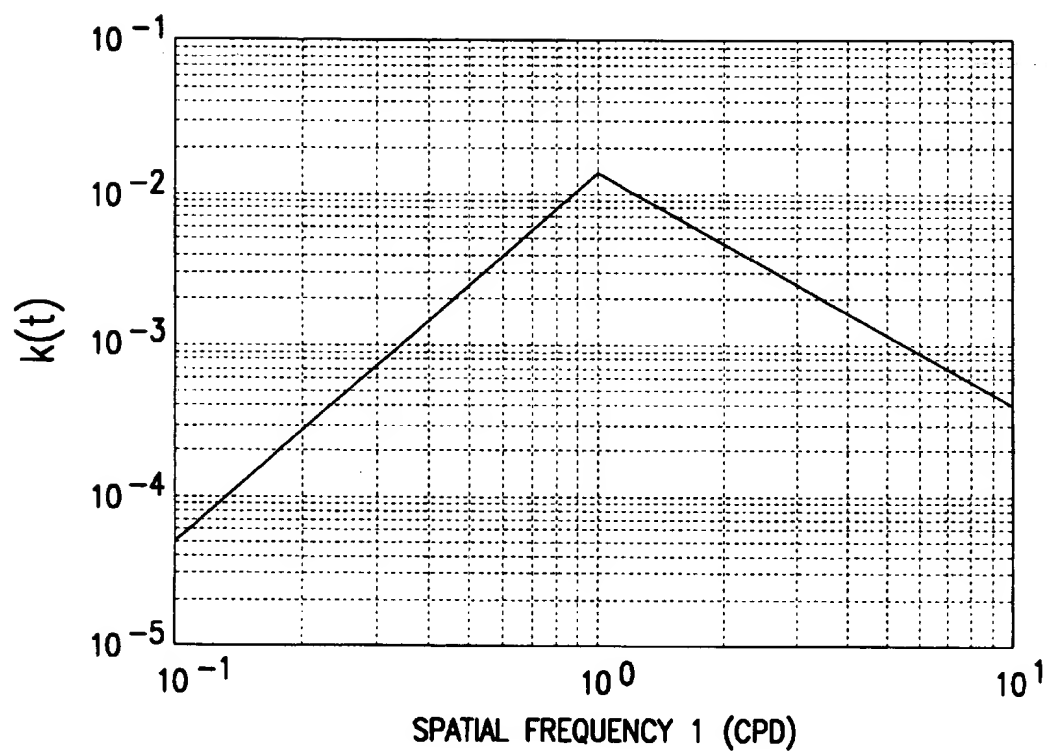


FIG. 5

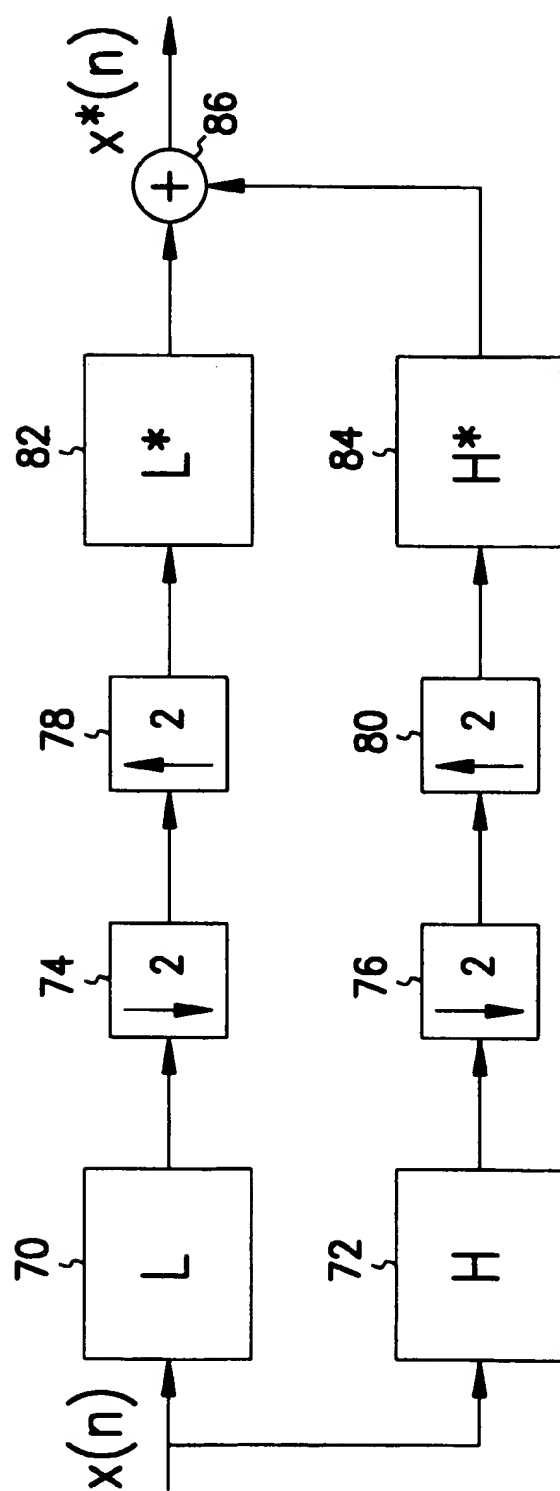


FIG. 6

METHOD AND APPARATUS FOR SCENE-BASED VIDEO WATERMARKING

RELATED DOCUMENTS

This application claims the benefit of U.S. Provisional Application No. 60/024,979, filed Aug. 30, 1996, which is hereby incorporated by reference. U.S. Provisional Application No. 60/050,587, filed Jun. 24, 1997, the benefit of which is also claimed, is also hereby incorporated by reference. Co-filed applications entitled "Method and Apparatus for Embedding Data, Including Watermarks, in Human Perceptible Sounds," Appl. Ser. No. 08/918,891, now U.S. Pat. No. 6,061,793, "Method and Apparatus for Embedding Data, Including Watermarks, in Human Perceptible Images," Appl. Ser. No. 08/918,122, now U.S. Pat. No. 6,031,914 and "Method and Apparatus for Video Watermarking," Appl. Ser. No. 08/918,125, and "Digital Watermarking to Resolve Multiple Claims of Ownership," Appl. Ser. No. 08/918,126 are also hereby incorporated by reference.

STATEMENT REGARDING GOVERNMENT RIGHTS

The present invention was made with government support by AFOSR under grant AF/F49620-94-1-0461, NSF grant INT-9406954, and AF/F49620-93-1-0558. The Government has certain rights in this invention.

FIELD OF THE INVENTION

This invention relates generally to techniques for embedding data such as watermarks, signatures and captions in digital data, and more particularly to scene-based watermarks in digital data that relates to video.

BACKGROUND OF THE INVENTION

Digital video is readily reproduced and distributed over information networks. However, these attractive properties lead to problems enforcing copyright protection. As a result, creators and distributors of digital video are hesitant to provide access to their digital intellectual property. Digital watermarking has been proposed as a means to identify the owner and distribution path of digital data. Digital watermarks address this issue by embedding owner identification directly into the digital data itself. The information is embedded by making small modifications to the pixels in each video frame. When the ownership of a video is in question, the information can be extracted to completely characterize the owner or distributor of the data.

Video watermarking introduces issues that generally do not have a counterpart in images and audio. Video signals are highly redundant by nature, with many frames visually similar to each other. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks, including frame averaging, frame dropping, interpolation, statistical analysis, etc. Many of these attacks may be accomplished with little damage to the video signal. A video watermark must handle such attacks. Furthermore, it should identify any image created from one or more frames in the video.

Furthermore, to be useful, a watermark must be perceptually invisible, statistically undetectable, robust to distortions applied to the host video, and able to resolve multiple ownership claims. Some watermarking techniques modify spatial/temporal data samples, while others modify transform coefficients. A particular problem afflicting all prior art

techniques, however, is the resolution of rightful ownership of digital data when multiple ownership claims are made, i.e., the deadlock problem. Watermarking schemes that do not use the original data set to detect the watermark are most vulnerable to deadlock. A pirate simply adds his or her watermark to the watermarked data. It is then impossible to establish who watermarked the data first.

Watermarking procedures that require the original data set for watermark detection also suffer from deadlocks. In such schemes, a party other than the owner may counterfeit a watermark by "subtracting off" a second watermark from the publicly available data and claim the result to be his or her original. This second watermark allows the pirate to claim copyright ownership since he or she can show that both the publicly available data and the original of the rightful owner contain a copy of their counterfeit watermark.

There is a need, therefore, for watermarking procedures applicable to video digital data that do not suffer from the described shortcomings, disadvantages and problems.

SUMMARY OF THE INVENTION

The above-identified shortcomings, disadvantages and problems found within the prior art are addressed by the present invention, which will be understood by reading and studying the following specification. The invention provides for the scene-based watermarking of video data.

In one embodiment of the invention, scenes are extracted from video host data that is made up of a number of successive frames. Each scene thus includes a number of frames. Each frame undergoes a wavelet transformation, which is then segmented into blocks. A frequency mask is applied to the corresponding frequency-domain blocks, which is then weighted with the author signature, also in the frequency domain. The resulting weighted block is taken out of the frequency domain, and then weighted with the spatial mask for its corresponding wavelet transformed block. A unique watermark generation routine is also described that assists in the resolution of deadlock.

The approach of the invention provides advantages over the approaches found in the prior art. In the prior art, an independent watermark applied to each frame may result in detection of the watermark by statistically comparing or averaging similar regions and objects in successive video frames, as has been described in the background. However, the inventive scene-based approach addresses this issue by embedding a watermark this is a composite of static and dynamic components, the dynamic components preventing detection by statistical comparison across frames. Therefore, statistical comparison or averaging does not yield the watermark.

Further aspects, advantages and embodiments of the invention will become apparent by reference to the drawings, and by reading the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flowchart of a method of a video watermarking process according to an embodiment of the invention;

FIG. 2 is a flowchart of a method of an object-based video watermarking process according to an embodiment of the invention;

FIG. 3 is a diagram of a typical computer to be used with embodiments of the invention;

FIG. 4 is a block diagram of a specific implementation of scene-based video watermarking, based on the methods of FIG. 1 and FIG. 2, according to an embodiment of the invention;

3

FIG. 5 is a diagram showing a masking weighting function $k(f)$ according to one embodiment of the invention; and,

FIG. 6 is a diagram showing a two-band perfect reconstruction filter in accordance with which a wavelet transform can be computed according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific preferred embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical and electrical changes may be made without departing from the spirit and scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense.

Overview of the Watermarking Process

Referring to FIG. 1, a flowchart of a method of a video watermarking process, according to one embodiment of the invention, is shown. Specifically, the method of FIG. 1 imbeds watermark data into host video data. In step 10, the watermark data is generated, which is the signature, or watermark, that acts as a unique identifier for the host video data. Note that the signature inherently is spread across the frequency spectrum without explicit spread-spectrum processing.

In one embodiment of the invention, the signature is a pseudo-random sequence, which is created using a pseudo-random generator and two keys. With the two proper keys, the watermark may be extracted. Without the two keys, the data hidden in the video is statistically invisible and impossible to recover. Pseudo-random generators are well within the art. For example, the reference R. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science* (J. van Leeuwen, ed.), vol. 1, ch. 13, pp. 717-755, Cambridge, Mass.: MIT Press, 1990, which is hereby incorporated by reference, describes such generators.

In one embodiment, the creation of the watermark data in step 10 works as follows. The author has two random keys x_1 and x_2 (i.e., seeds) from which the pseudo-random sequence y can be generated using a suitable cryptographic operator $g(x_1, x_2)$, as known within the art. The noise-like sequence y , after some processing, is the actual watermark hidden into the video stream. The key x_1 is author dependent. The key x_2 is signal dependent. In particular, x_1 is the secret key assigned to (or chosen by) the author. Key x_2 is computed from the video signal which the author wishes to watermark. The signal dependent key is computed from the masking values of the original signal. The masking values give us tolerable error levels in the host video signal. The tolerable error levels are then hashed to a key x_2 .

The operator $g(\)$ is called a pseudo-random sequence generator. For the pseudo-random generator to be useful, a pirate must not be able to predict bits of y or infer the keys x_1 or x_2 from knowledge of some bits of y . There are several popular generators that satisfy these properties, including RSA, Rabin, Blum/Micali, and Blum/Blum/Shub, as known within the art. For example, the Blum/Blum/Shub pseudo-random generator uses the one way function $y=g(x)=x^2 \bmod n$, where $n=pq$ for primes p and q so that $p=q=3 \bmod 4$.

4

It can be shown that generating x or y from partial knowledge of y is computationally infeasible for the Blum/Blum/Shub generator. The classical maximal length pseudo noise sequence (i.e., m-sequence) generated by linear feedback shift registers are not used for this purpose. Sequences generated by shift registers are cryptographically insecure, as one can solve for the feedback pattern (i.e., the keys) given a small number of output bits y .

Thus, a pirate is not free to subtract off a second watermark y' arbitrarily. The pirate must supply the keys x_1' and x_2' which generate the watermark y' they wish to embed. It is computationally infeasible to invert the one-way function $y=g(x_1', x_2')$ to obtain x_1' and x_2' . Furthermore, x_2' is not arbitrary. It is computed directly from the original video signal, which is inaccessible to the pirate. As a result, the two-key pseudo-random sequence author representation resolves the deadlock problem.

In step 11, a wavelet transform is applied along the temporal axis of the video host data, resulting in a multi-resolution temporal representation of the video. In particular, the representation consists of temporal lowpass frames and highpass frames. The lowpass frames consist of the static components in the video scene. The highpass frames capture the motion components and changing nature of the video sequence (i.e., the video host data). The watermark is designed and embedded in each of these components. The watermarks embedded in the lowpass frames exist throughout the entire video scene. The watermarks embedded in the motion frames are highly localized in time and change rapidly from frame to frame. Thus, the watermark is a composite of static and dynamic components. The combined representation overcomes drawbacks associated with a fixed or independent watermarking procedure. (i.e., avoidance of watermark detection by statistical comparison between successive frames is achieved.)

A wavelet transform can be computed using a two-band perfect reconstruction filter bank as shown in FIG. 6. The video signal is simultaneously passed through lowpass L filter 70 and highpass H filter 72 and then decimated by 2 (as represented by elements 74 and 76 of FIG. 6) to give static (no motion) and dynamic (motion) components of the original signal. The two decimated signals may be up sampled (as represented by elements 78 and 80), and then passed through complementary filters 82 and 84 and summed as represented by element 86 to reconstruct the original signals. Wavelet filters are widely available within the art. For instance, the reference P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Englewood Cliffs, N.J.: PTR Prentice-Hall, Inc., 1992, which is hereby incorporated by reference, describes such filters.

Referring back to FIG. 1, in step 12, the data generated by step 10 is imbedded into a perceptual mask of the host video data as represented by the temporal wavelet transform of step 11. The present invention employs perceptual masking models to determine the optimal locations within host data in which to insert the watermark. The perceptual mask is specific to video host data. The mask provides for the watermark data generated by step 10 to be embedded with the host data, at places typically imperceptible to the human eye. That is, the perceptual mask exploits masking properties of the human visual system. Step 12 embeds the watermark within the temporally wavelet transformed host data such that they will not be perceived by a human eye, as defined by the perceptual model. The perceptual masking of step 12 is conducted in the frequency domain.

Thus, image masking models based on the human visual system (HVS) are used to ensure that the watermark embed-

5

ded into each video frame is perceptually invisible and robust. Visual masking refers to a situation where a signal raises the visual threshold for other signals around it. Masking characteristics are used in high quality low bit rate coding algorithms to further reduce bit rates. The masking models presented here are based on image models.

The masking models give the perceptual tolerance for image coefficients and transform coefficients. These masking models are also described in the reference B. Zhu, et al., "Low Bit Rate Near-Transparent Image Coding," in Proc. of the SPIE Int'l Conf. on Wavelet Apps. for Dual Use, vol. 2491, (Orlando, Fla.), pp. 173-184, 1995, which is hereby incorporated by reference, and in the reference B. Zhu, et al., "Image Coding with Mixed Representations and Visual Masking," in Proc. 1995 IEEE Int'l Conf. on Acoustics, Speech and Signal Processing, (Detroit, Mich.), pp. 2327-2330, 1995, which is also hereby incorporated by reference. The frequency masking model is based on the knowledge that a masking grating raises the visual threshold for signal gratings around the masking frequency. The model is based on the discrete cosine transform (DCT), expresses the contrast threshold at frequency f as a function of f , the masking frequency f_m and the masking contrast cm :

$$c(f, f_m) = c_d(f) \cdot \text{Max}\{1, [k(f/f_m)cm]^p\},$$

where $c_d(f)$ is the detection threshold at frequency f . The mask weighting function $k(f)$ is shown in FIG. 5. To find the contrast threshold $c(f)$ at a frequency f in an image, the DCT is first used to transform the image into the frequency domain and find the contrast at each frequency. The value $\alpha=0.62$ as determined experimentally by psycho-visual tests, and as described in G. E. Legge and J. M. Foley, "Contrast Masking in Human Vision," Journal Optics Society of America, vol. 70, no. 12, pp. 1458-1471 (1980), which is hereby incorporated by reference. Then, a summation rule of the form

$$c(f) = [\sum f_m c(f, f_m)]^{1/\alpha},$$

is used to sum up the masking effects from all the masking signals near f . If the contrast error at f is less than $c(f)$, the model predicts that the error is invisible to human eyes.

In step 14, the host video data as subjected to a temporal wavelet transform in step 11, with the embedded watermark data from step 12 is further subjected to a non-frequency mask. Because the perceptual mask in step 12 is a frequency domain mask, a further mask is necessary to ensure that the embedded data remains invisible in the host video data. The non-frequency mask is a spatial mask.

Frequency masking effects are localized in the frequency domain, while spatial masking effects are localized in the spatial domain. Spatial masking refers to the situation that an edge raises the perceptual threshold around it. Any model for spatial masking can be used, and such models are well known in the art. However, the model used in one embodiment of the invention is similar to the model described in the Zhu, "Low Bit Rate . . ." reference previously incorporated by referenced, and which is itself based on a model proposed by Girod in "The Information Theoretical Significance of Spatial and Temporal Masking in Video Signals," in Proceedings of the SPIE Human Vision, Visual Processing, and Digital Display, vol. 1077, pp. 178-187 (1989), which is also herein incorporated by reference.

In one embodiment, the upper channel of Girod's model is linearized under the assumption of small perceptual errors, the model giving the tolerable error level for each pixel in

6

the image, as those skilled in the art can appreciate. Furthermore, under certain simplifying assumptions described in the Zhu "Bit Rate . . ." reference, the tolerable error level for a pixel $p(x,y)$ can be obtained by first computing the contrast saturation at (x,y)

$$dc_{sat}(x, y) = dc_{sat} = \sqrt{\frac{T}{\sum_{x', y'} w_d(0, 0, x', y')}}.$$

where the weight $w_d(x,y,x',y')$ is a Gaussian centered at the point (x,y) and T is a visual test based threshold. Once $dc_{sat}(x,y)$ is computed, the luminance on the retina, dl_{ret} , is obtained from the equation

$$dc_{sat}(x,y) = w_2(x,y) \cdot dl_{ret}(x,y)$$

From dl_{ret} , the tolerable error level $ds(x,y)$ for the pixel $p(x,y)$ is computed from

$$dl_{ret}(x,y) = w_1(x,y) \cdot ds(x,y)$$

The weights $w_1(x,y)$ and $w_2(x,y)$ are based on Girod's model. The masking model predicts that changes to pixel $p(x,y)$ less than $ds(x,y)$ introduce no perceptible distortion.

As have been described, steps 10, 11, 12 and 14 of FIG. 1 provide an overview of the video watermarking process of the present invention. An overview of the scene-based video watermarking process of the present invention is now described.

Overview of the Scene-Based Video Watermarking Process

Referring to FIG. 2, a flowchart of a method of a scene-based video watermarking process, according to one embodiment of the invention, is shown. The method utilizes the watermarking method of FIG. 1 already described. In step 24, a video sequence (i.e., the host video data) is broken (segmented) into scenes, as known within the art. For example, the reference J. Nam and A. H. Tewfik, "Combined Audio and Visual Streams Analysis for Video Sequence Segmentation," in Proceedings of the 1997 International Conference on Acoustics, Speech and Signal Processing, (Munich, Germany), pp. 2665-2668 (April 1997), which is hereby incorporated by reference, describes such scene segmentation. Segmentation into scenes allows the watermarking procedures to take into account temporal redundancy. Visually similar regions in the video sequence, e.g., frames from the same scene, must be embedded with a consistent watermark. The invention is not limited to a particular segmentation into scenes algorithm, however.

In step 26, a temporal wavelet transform is applied on the video scenes, as has been previously described. That is, each scene comprises a number of frames, such that a temporal wavelet transform is applied to each frame within a scene. The resulting frames are known as wavelet frames. The multiresolution nature of the wavelet transform allows the watermark to exist across multiple temporal scales, resolving pirate attacks. For example, the embedded watermark in the lowest frequency (DC) wavelet frame exists in all frames in the scene.

In step 28, a watermark is embedded in each wavelet frame. The watermark is designed and embedded in the wavelet domain, such that the individual watermarks for each wavelet frame are spread out to varying levels of support in the temporal domain. For example, watermarks embedded in highpass wavelet frames are localized tempo-

rally. Conversely, watermarks embedded in lowpass wavelet frames are generally located throughout the scene in the temporal domain. The watermarks are embedded in accordance with perceptual and non-frequency masks, as has been described. That is, the watermarks are embedded in each frame of each scene in accordance with perceptual and spatial (non-frequency) characteristics of the frame, as has been described in conjunction with the method of FIG. 1.

The scene-based video watermarking method of the invention has several other advantages. It is scene-based and video dependent, and directly exploits spatial masking, frequency masking, and temporal properties such that the embedded watermark is invisible and robust. The watermark consists of static and dynamic temporal components that are generated from a temporal wavelet transform of the video scenes. The resulting wavelet frames are modified by a perceptually shaped pseudo-random sequence representing the author (owner). The noise-like watermark is statistically undetectable to thwart unauthorized removal. Furthermore, the author representation resolves the deadlock problem. The multiresolution watermark may be detected on single frames without knowledge of the location of the frames in the video scene.

Because the video watermarking procedure is perception-based, the watermark adapts to each individual video signal. In particular, the temporal and frequency distributions of the watermark are controlled by the masking characteristics of the host video signal. As a result, the strength of the watermark increases and decreases with host, e.g., higher amplitude in regions of the video with more textures, edges, and motion. This ensures that the embedded watermark is invisible while having the maximum possible robustness.

Because the watermark representation is scene-based and multiscale, given one or more frames from a potentially pirated video, the watermark may be extracted from the frames without knowledge of the location of the frame being tested. This detection characteristic exists due to the combined static and dynamic representation of the watermark.

The watermark representation of the invention provides an author representation that solves the deadlock problem. The author or owner of the video is represented with a pseudo-random sequence created by a pseudo-random generator and two keys. One key is author dependent, while the second key is signal dependent. The representation is able to resolve rightful ownership in the face of multiple ownership claims.

The watermark representation of the invention also provides a dual watermark. The watermarking scheme uses the original video signal to detect the presence of a watermark. The procedure can handle virtually all types of distortions, including cropping, temporal resealing, frame dropping, etc., using a generalized likelihood ratio test. This procedure is integrated with a second watermark which does not require the original signal to address the deadlock problem.

As have been described, steps 24, 26, and 28 of FIG. 2 provide an overview of the scene-based watermarking process of the present invention. The specifics of the hardware implementation of the invention are now provided.

Hardware Implementation of the Invention

The present invention is not limited as to the type of computer on which it runs. However, a typical example of such a computer is shown in FIG. 3. Computer 16 is a desktop computer, and may be of any type, including a PC-compatible computer, an Apple Macintosh computer, a UNIX-compatible computer, etc. Computer 16 usually

includes keyboard 18, display device 20 and pointing device 22. Display device 20 can be any of a number of different devices, including a cathode-ray tube (CRT), etc. Pointing device 22 as shown in FIG. 3 is a mouse, but the invention is not so limited. Not shown is that computer 16 typically also comprises a random-access memory (RAM), a read-only memory (ROM), a central-processing unit (CPU), a fixed storage device such as a hard disk drive, and a removable storage device such as a floppy disk drive. The computer program to implement the present invention is typically written in a language such as C, although the present invention is not so limited.

The specifics of the hardware implementation of the invention have been described. A particular implementation of the scene-based video watermarking of the invention, based on the methods of FIG. 1 and FIG. 2, is now described.

Particular Implementation of Scene-Based Video Watermarking

The embodiment shown in FIG. 4 illustrates a particular implementation of scene-based video watermarking according to the invention, as based on the methods of FIG. 1 and FIG. 2 that have already been described. Referring now to FIG. 4, a block diagram of this specific implementation of scene-based video watermarking is shown. Video frames 32 (of video host data) are denoted such that F_i is the i th frame in a video scene, where $i=0, \dots, k-1$. Frames are ordered sequentially according to time. Each frame is of size $n \times m$. The video itself may be gray scale (8 bits/pixel) or color (24 bits/pixel). Frames 32 undergo a temporal wavelet transformation 34, as has been described, to become wavelet frames 36. The tilde representation is used to denote a wavelet representation. For example, $F_{\sim i}$ is the i th wavelet coefficient frame. Without loss of generality, wavelet frames are ordered from lowest frequency to highest frequency—i.e., $F_{\sim 0}$ is a DC frame. Thus, there are k wavelet coefficient frames $F_{\sim i}$, $i=0, \dots, k-1$.

In step 38, each wavelet frame $F_{\sim i}$ is segmented into 8×8 blocks $B_{\sim ij}$, $i=0, 1, \dots, (n/8)$ and $j=0, 1, \dots, (m/8)$. In step 40, each block $B_{\sim ij}$ is subjected to a discrete cosine transform (DCT), to become block $B'_{\sim ij}$. In step 42, a perceptual frequency mask, as has been described, is applied to each block to obtain the frequency mask M'_{ij} . In step 44, author signature Y_{ij} —the watermark—also undergoes a discrete cosine transform to become Y'_{ij} . It should be noted that the generation of author signature Y_{ij} is desirably in accordance with the process that has been described in conjunction with step 10 of FIG. 1, but the invention is not so limited.

In step 46, the mask M'_{ij} is used to weight the noise-like author Y'_{ij} for that frame block, creating the frequency-shaped author signature $P'_{ij}=M'_{ij}Y'_{ij}$. In step 48, the spatial mask $S_{\sim ij}$ is generated, as has been described, and in step 50, the wavelet coefficient watermark block $W_{\sim ij}$ is obtained by computing the inverse DCT of P'_{ij} in step 52 and locally increasing the watermark to the maximum tolerable error level provided by the spatial mask $S_{\sim ij}$. Finally, in step 54, the watermark $W_{\sim ij}$ is added to the block $B_{\sim ij}$, creating the watermarked block. The process is repeated for each wavelet coefficient frame $F_{\sim i}$.

The watermark for each wavelet coefficient frame is the block concatenation of all the watermark blocks for that frame. The wavelet coefficient frames with the embedded watermarks are then converted back to the temporal domain using the inverse wavelet transform. As the watermark is designed and embedded in the wavelet domain, the individual watermarks for each wavelet coefficient frame are

spread out to varying levels of support in the temporal domain. For example, watermarks embedded in highpass wavelet frames are localized temporally. Conversely, watermarks embedded in lowpass wavelet frames are generally located throughout the scene in the temporal domain.

The watermarks embedded within the video data according to the method of FIG. 4 should be extractable even if common signal processing operations are applied to the host data. This is particularly true in the case of deliberate unauthorized attempts to remove the watermark. For example, a pirate may attempt to add noise, filter, code, re-scale, etc., the host data in an attempt to destroy the watermark. The embedded watermark, however, is noise-like and its location over multiplied blocks of the host data, over successive frames of the data, is unknown. Therefore, the pirate has insufficient knowledge to directly remove the watermark. Furthermore, a different signature is used for each block to further reduce unauthorized watermark removal by cross correlation. Any destruction attempts are done blindly.

Detection of the watermark is accomplished via generalized likelihood ratio test. Two methods have been developed to extract the potential watermark from a test video or test video frame. Both employ hypothesis testing. One test employs index knowledge during detection, i.e., the placement of the test video frame(s) relative to the original video is known. The second detection method does not require knowledge of the location of the test frame(s). This is extremely useful in a video setting, where 1000's of frames may be similar, and it is uncertain where the test frames reside.

In the first method, watermark detection with index knowledge, when the location of the test frame is known, a straightforward hypothesis test may be applied. For each frame in the test video R_k , a hypothesis test is performed.

$H_0: X_k = R_k - F_k = N_k$ (no watermark)

$H_1: X_k = R_k - F_k = W^*k + N_k$ (watermark)

where F_k is the original frame, W^*k is the (potentially modified) watermark recovered from the frame, and N_k is noise. The hypothesis decision is obtained by computing the scalar similarity between each extracted signal and original watermark W_k : $S_k = \text{Simk}(X_k, W_k) = (X_k^*W_k)/(W_k^*W_k)$. The overall similarity between the extracted and original watermark is computed as the mean of S_k for all k : $S = \text{mean}(S_k)$. The overall similarity is compared with a threshold to determine whether the test video is watermarked. The experimental threshold is desirably chosen around 0.1, i.e., a similarity value ≥ 0.1 indicates the presence of the owner's copyright. In such a case, the video is deemed the property of the author, and a copyright claim is valid. A similarity value < 0.1 indicates the absence of a watermark.

When the length (in terms of frames) of the test video is the same as the length of the original video, the hypothesis test is performed in the wavelet domain. A temporal wavelet transform of the test video is computed to obtain its wavelet coefficient frames $R \sim k$. Thus,

$H_0: X \sim k = R \sim k - F \sim k = N_k$ (no watermark)

$H_1: X \sim k = R \sim k - F \sim k = W \sim k + N_k$ (watermark)

where $F \sim k$ are the wavelet coefficient frames from the original video, $W \sim k$ is the potentially modified watermarks from each frame, and N_k is noise. This test is performed for each wavelet frame to obtain $X \sim k$ for all k . Similarity values are computed as before, $S_k = \text{Simk}(X \sim k, W \sim k)$.

Using the original video signal to detect the presence of a watermark, virtually all types of distortions can be handled, including cropping, rotation, resealing, etc., by

employing a generalized likelihood ratio test. A second detection scheme which is capable of recovering a watermark after many distortions without a generalized likelihood ratio test has also been developed. The procedure is fast and simple, particularly when confronted with the large amount of data associated with video.

In the method for watermark detection without index knowledge, there is no knowledge of the indices of the test frames. Pirate tampering may lead to many types of derived videos which are often difficult to process. For example, a pirate may steal one frame from a video. A pirate may also create a video which is not the same length as the original video. Temporal cropping, frame dropping, and frame interpolation are all examples. A pirate may also swap the order of the frames. Most of the better watermarking schemes currently available use different watermarks for different images. As such, they generally require knowledge of which frame was stolen. If they are unable to ascertain which frame was stolen, they are unable to determine which watermark was used.

This method can extract the watermark without knowledge of where a frame belongs in the video sequence. No information regarding cropping, frame order, interpolated frames, etc., is required. As a result, no searching and correlation computations are required to locate the test frame index. The hypothesis test is formed by removing the low temporal wavelet frame from the test frame and computing the similarity with the watermark for the low temporal wavelet frame. The hypothesis test is formed as

$H_0: X_k = R_k - F \sim 0 = N_k$ (no watermark)

$H_1: X_k = R_k - F \sim 0 = W \sim k + N_k$ (watermark)

where R_k is the test frame in the spatial domain and $F \sim 0$ is the lowest temporal wavelet frame. The hypothesis decision is made by computing the scalar similarity between each extracted signal X_k and original watermark for the low temporal wavelet frame $W \sim 0$: $\text{Simk}(X_k, W \sim 0)$. This simple yet powerful approach exploits the wavelet property of varying temporal support.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.

I claim:

1. A computerized method for embedding data representing a watermark into host data relating to video:

generating the data representing the watermark;
subjecting the host data to a temporal wavelet transform;
embedding the data into the host data, as subjected to the temporal wavelet transform, in accordance with a perceptual mask conducted in the frequency domain; and,
subjecting the host data, including the data embedded therein, to a non-frequency mask.

2. The computerized method of claim 1, wherein the data representing the watermark comprises a pseudo-random sequence.

3. The computerized method of claim 1, wherein generating the data representing the watermark uses a pseudo-random generator and two keys to generate the data.

4. The computerized method of claim 3, wherein the pseudo-random generator is selected from the group comprising RSA, Rabin, Blum/Micali, and Blum/Blum/Shub.

5. The computerized method of claim 1, wherein the perceptual mask comprises a model in which a contrast

11

threshold at a frequency f is expressed as a function of the frequency f , a masking frequency f_m and a masking contrast c_m ,

$$c(f, f_m) = c_d(f) \cdot \text{Max}\{1, [k(f/f_m)c_m]^p\}, \quad 5$$

where $c_d(f)$ is a detection threshold at the frequency f .

6. The computerized method of claim 1, wherein the non-frequency mask comprises a spatial mask.

7. The computerized method of claim 1, wherein subjecting the host data to a temporal wavelet transform results in a multiresolution temporal representation of the video having temporal lowpass frames and temporal highpass frames. 10

8. A scene-based computerized method of watermarking host data relating to video comprising:

segmenting the host data into a plurality of scenes, each scene having a plurality of frames; 15

subjecting each frame of each scene to a temporal wavelet transform; and,

embedding each frame of each scene, as has been subjected to the temporal wavelet transform, with a watermark in accordance with perceptual and spatial characteristics of the frame. 20

9. The scene-based computerized method of claim 8, wherein subjecting each frame of each scene to the temporal wavelet transform results in lowpass wavelet frames and highpass wavelet frames. 25

10. The scene-based computerized method of claim 9, wherein watermarks embedded in lowpass wavelet frames are located throughout the scene in a temporal domain. 30

11. The scene-based computerized method of claim 9, wherein watermarks embedded in highpass wavelet frames are localized temporally.

12. A computerized system for watermarking host data relating to video and having a plurality of scenes, each scene having a plurality of frames, comprising: 35

a processor;

a computer-readable medium;

computer-executable instructions executed by the processor from the computer-readable medium comprising: 40
applying a temporal wavelet transform to each frame;
segmenting each frame of each scene into blocks;

12

applying a discrete cosine transform (DCT) to each block to generate a frequency block corresponding to the block;

generating a perceptual mask for each frequency block; applying the DCT to a watermark for each frequency block;

weighting the perceptual mask for each frequency block with the watermark for the frequency block to which the DCT has been applied to generate a frequency-shaped author block;

applying an inverse DCT to each frequency-shaped author block to generate a time-domain block;

generating a spatial mask for each block; weighting each time-domain block by a spatial mask to generate a watermark block; and,

adding each block to a corresponding watermark block to generate a watermarked block.

13. A computer-readable medium having a computer program stored thereon to cause a suitable equipped computer to perform a method comprising:

applying a temporal wavelet transform to each frame;

segmenting each frame of each scene into blocks;

applying a discrete cosine transform (DCT) to each block to generate a frequency block corresponding to the block;

generating a perceptual mask for each frequency block; applying the DCT to a watermark for each frequency block;

weighting the perceptual mask for each frequency block with the watermark for the frequency block to which the DCT has been applied to generate a frequency-shaped author block;

applying an inverse DCT to each frequency-shaped author block to generate a time-domain block;

generating a spatial mask for each block;

weighting each time-domain block by a spatial mask to generate a watermark block; and,

adding each block to a corresponding watermark block to generate a watermarked block.

14. The computer-readable medium of claim 13, wherein the computer-readable medium is a floppy disk.

* * * * *